EXHIBIT 4

Acceptable Use Policy

KB0018310
6375 views

Acceptable Use Policy

ISSUING OFFICE

Information Services

POLICY

The information systems of Liberty University, Inc. ("**Liberty**" of the "**University**") are intended for the use of authorized members of the Liberty community in furtherance of their academic and administrative work. Liberty's information systems consist of all networking, computing and telecommunications wiring, equipment, networks, security devices, passwords, servers, computer systems, computers, computer laboratory equipment, workstations, Internet connection(s), electronic mail services, television and radio technologies, University-owned mobile communication devices and all other intermediary equipment, services and facilities (hereafter referred to as "**Information Systems**"). These assets are the property of the University.

Users of the University's Information Systems are expected to review, understand, and comply to this Policy and its associated standards.

STANDARDS

User Rights and Responsibilities

Assent to Terms of the Acceptable Use Policy

Every individual who accesses and/or uses the Information Systems, whether by "clicking through" usage agreement during sign-on to any University system, registration onto Liberty's network or any other equipment registration procedure, is deemed to assent to and must comply with this Policy.

Access To and Use of Systems/Normal Duration of Service

Access to and use of the Information Systems is a privilege granted by the University to faculty, staff, students, their approved guests, and other authorized third parties, in University's sole discretion ("Users"). The University retains sole discretion over the extent to which access privileges are granted, extended, and/or revoked.

Use of Computer Accounts and Facilities

Users may use only the Information Systems for their individual use. Use of another person's account, identity, security devices/tokens, or presentment of false or misleading information or credentials, or unauthorized use of Information Systems is prohibited.

Behavior of all users on the network must be consistent with all applicable University policies including the University's Mission and Doctrinal Position, and in accordance with The Liberty Way (for resident students), The Liberty Way Online Honor Code (for Online students), Faculty Handbook (for Residential faculty), The LU Online Faculty Handbook (for Online faculty, currently under review), and The Employee Handbook (for staff).

The University is not responsible or liable for any personal or unauthorized use of Information Systems.

Management of Assigned Information Systems

Users will allow Information Systems assigned to them to be managed via Information Services to ensure that their systems are kept up to date. Information Services is only responsible for updating University-provided software installed by IT Endpoint Device Management, unless otherwise approved by the IS Account Management & Compliance Office.

Users are not permitted to install additional third-party software on Information Systems except as otherwise provided by IS Accounts Management & Compliance Office. Users are personally responsible for all third-party software installed on Information Systems, even if Information Services assists in its installation. Prior to installing any third-party software, Users must ensure that such software is not prohibited on University's Information Systems and that all required licenses are obtained. Users must ensure that all third-party software is kept up to date, including security patches. Any software discovered on Information Systems that is not in compliance with this Policy (such as violation of valid licensing) may be blocked/removed remotely or automatically as part of routine maintenance in University's sole discretion without notice and result in User discipline as provided below.

All third-party software must be properly licensed. Each user is personally responsible for all software not installed by IT Endpoint Device Management or approved by the IS Accounts Management & Compliance office.

Users Responsible for Actions Conducted Under their User ID(s)

Users are responsible for all use of Information Systems conducted under their unique, University-provided credentials, and are expected to take reasonable precautions, including

password security and file protection measures, to prevent use of their accounts and files by unauthorized persons/entities. Sharing of passwords or other access tokens with others is prohibited. Users who disclose their passwords to third parties are solely responsible for all consequences arising from such disclosure. You have a responsibility to promptly report the theft, loss or unauthorized use of your accounts to your supervisor or the Director of Information Security. If you discover a possible security issue related to University systems, report the problem immediately to IT Helpdesk. IT Helpdesk can be reached at (866)-447-2869 or (434)-592-7800.

University Approved Communication Methods

Electronic communications pertaining to the official business of the University, including all academic and administrative matters, which are transmitted using Information Systems must be sent via University-approved messaging systems (i.e., Microsoft Outlook and Teams) using the sender's unique University-provided account associated with a University-recognized e-mail system. Third party messaging systems (e.g., Signal, discord, text, and non-University email accounts) are not recognized by the University as approved methods of communication for University business on Information Systems.

The University owns all University email accounts and data transmitted or stored using the University email account. Forwarding LU emails that contain high-risk information is not permissible. Automation tools or protocols to enable auto-forwarding moving University managed emails to a non-university-managed email system is not permitted. Personal email accounts or servers set up to receive University emails or messaging is not permitted. Upon separation of employment from the University, faculty and staff who are not University alumni will no longer have access to their University email account.

Email accounts assigned to a user by LU are a privilege and should not be misused. Misuse of an email account could result in the suspension of the account. Each user is responsible for protecting your password, any other security mechanisms the university provides you. If you think your password has been stolen or someone has used your account or access, report it immediately to the Help Desk.

Posting of Personal Information/Web Pages/Other Electronic Writings

Users are responsible for the timeliness, accuracy, and content/consequences of their personal information, web pages and other electronic writings transmitted using Information Systems. Users may not publish personal information of members of the Liberty community, including, but not limited to students, faculty and staff, may not be posted or maintained on public networks or sites, unless the User fully complies with all University policies, procedures, and applicable laws and regulations governing handling of personal information.

Use of University-Recognized Messaging Systems

Electronic messages pertaining to the official business of the University, including all academic and administrative matters should be sent from University-owned or University-recognized messaging systems. For example, inquiries about students must be sent from an account associated with a University-recognized e-mail system. Replies from faculty or staff must be sent using the same University-recognized accounts. In cases where unrecognized third-party messaging systems are used to originate a message, and/or where a party chooses to forward messages from a University-owned or University-recognized system to a third-party unrecognized system, individuals using these systems will be solely responsible for all consequences arising from such use.

Commercial Use

University Information Systems may not be used for commercial purposes not related to the University's business operations, academic, research, and scholarly pursuits except as permitted with the explicit prior written approval of the Chief Information Officers.

Offering, Providing, Lending or Renting Access to University Systems

Users may not offer, provide, lend, rent or sell access to University Information Systems. Users may not provide access to individuals outside the University community. Expansion or redistribution of Liberty's cable television services is not permitted. Personal, private or departmental switches, routers, wireless access points or DHCP-serving devices may not be connected to centrally managed administrative network segments, except only as may be agreed to in writing between the device owner and Information Technology Services.

Compliance with Internet Service Provider Terms of Use

Internet use must comply with the Terms of Service stipulated by our Internet service provider(s). In addition, the Acceptable Use, Terms of Service and/or other policies of systems and/or electronic resources accessed through University Internet connection(s) also bind users of University Internet connections. Failure of users to comply with these Terms of Service may result in sanctions, up to and including separation from the University.

Use of Remote Resources

Users may not use Information Systems to connect to remote resources regardless of location on or off the Liberty network, unless otherwise approved in advance by the IS Accounts Management & Compliance Office and the administrator of the remote resource.

All access to Information Systems must occur through reasonable and customary means. For example, all electronic resources offered through a web-based experience should be accessed using a web browser only.

Electronic resources are available to faculty and staff using "remote access," also known as the Virtual Private Network (VPN). The University reserves and intends to exercise its right to determine:

· who may use the VPN,

· what devices may access the VPN,

· from what locations the VPN may be accessed,

· what services and experiences are offered through the VPN,

· the extent of individual access rights when using the VPN, and

· to limit or block connections not originating from the VPN.

Exclusions to this policy provision may be made to vendors and affiliates who maintain private connections to the University network.

All users establishing a connection to the University network through the VPN or by any other means are responsible to ensure antivirus software is present on their computer, and that its protection signatures are up to date, and that the operating system is a current and supported version that has received available software and security updates.

The use of the University's VPN services on personally owned or non-Liberty University managed devices is not permitted unless approved by the CIO office.

Irresponsible/Wasteful Use

Users may not use Information Systems irresponsibly, wastefully or in a manner that adversely affects the work or equipment of others at Liberty or on the Internet, as determined by the University in its sole discretion.

Specific Prohibitions on Use of Information Systems

· Harass, threaten, defame, slander or intimidate any individual or group;

· Generate and/or spread intolerant or hateful material, which in the sole judgment of the University is directed against any individual or group, based on race, religion, national origin, ethnicity, age, gender, marital status, sexual orientation, veteran status, genetic makeup, or disability;

· Transmit or make accessible material, which in the sole judgment of the University is offensive, violent, pornographic, annoying or harassing, including use of Liberty Information Systems to access and/or distribute obscene or sexually explicit material unrelated to University sanctioned work or bona fide scholarship;

· Generate unsolicited electronic mail such as chain messages, unsolicited job applications or commercial announcements;

· Generate falsely identified messages or content, including use of forged content of any description;

· Transmit or make accessible password information;

· Attempt to access Information Systems and/or resources for which authority has not been explicitly granted by the system owner(s);

· Capture, decipher or record user IDs, passwords, or keystrokes;

· Manipulate or tamper with uniform resource locators (URLs);

· Intercept electronic communications of any kind;

· Probe by any means the security mechanisms of any resource on the Liberty network, or on any other network through a connection to the Liberty network;

· Disclose or publish by any means the means to defeat or disable the security mechanisms of any component of a Liberty University Information System or network:

· Alter, degrade, damage or destroy data;

· Conduct illegal, deceptive or fraudulent activity;

· Obtain, use or retransmit copyrighted information without permission of the copyright holder;

· Engage in crypto-currency mining using Liberty electronic or network resources;

· Communicate in a manner that could be utilized for academic cheating;

· Place bets, wagers or operate games of chance; or

· Tax, overload, impede, interfere with, damage or degrade the normal functionality, performance or integrity of any device, service or function of Liberty Information Systems, content, components, or the resources of any other electronic system, network, service or property of another party, corporation, institution or organization.

The above enumeration is not all-inclusive. If there is a question as to whether a specific use is appropriate or acceptable under this policy, the University's sole determination will prevail. For additional information, contact the HelpDesk.

University Rights and Responsibilities

General Rights of the University

To protect the Information Systems against unauthorized or improper use, and to protect Users from the effects of unauthorized or improper usage, the University reserves the right with or without notice, to monitor, record, limit or restrict any user account, access and/or usage of account. The University may also monitor, record, inspect, copy, remove or otherwise alter any data, file or system resources in its sole discretion. The University further reserves the right to periodically inspect systems and take any other actions necessary to protect its Information Systems. The University also retains access rights to all files and electronic mail on its Information Systems. Anyone using these systems expressly consents to such monitoring.

Right to Seize/Inspect University-Owned Computing Devices

The University reserves the right at any time, with or without prior notice or permission from the user or users of a computer or other University-owned computing device, to seize such device and/or copy or have copied, any and all information from the data storage mechanisms of such

device as may be required in the sole discretion of the University in connection with investigations of possible wrongdoing or legal action. In addition to the foregoing, privately owned devices connected to the University network are also subject to inspection by authorized University personnel.

Right to Block Content

The University reserves the right to reject from the network or block electronic communications and content deemed not to be in compliance with policies governing use of University Information Systems.

Right to Disclosure Information

The University may disclose information, including pursuant to an internal or external investigation of alleged misconduct or wrongdoing, and may provide information to third parties, including law enforcement. By accessing the Information Systems, users give Liberty permission to conduct each of the operations described above.

Detection of Plagiarism/Academic Dishonesty

The University reserves the right to use, and intends to use manual and/or automated means to assess materials submitted as academic work submitted electronically for indications of plagiarism or other form(s) of academic dishonesty.

Actions to be Taken When a Policy Violation is Identified

When a potential violation is identified, the appropriate system manager or unit head, the Information Security Office, and any other University employees or agents as are deemed appropriate, are authorized to investigate and initiate action in accordance with University policy. Repeated violations may result in suspension or termination of service(s). In addition, the University may require restitution for any use of Information Systems that violates this policy. The University may also provide evidence of possible illegal or criminal activity to law enforcement authorities.

Noncompliance to these standards will be subject to disciplinary actions outlined in the academic honor code and personal conduct that applies to them, such as The Liberty Way, Residential Graduate Honor Code and LU Online Code of Honor (for students), the Faculty Staff Handbook or the LU Online Faculty Handbook (for faculty) and/or the Employee Handbook (for staff).

Noncompliance to these standards by any guest may result in the revocation of all access to Liberty University computing resources.

Consequences of Policy Violation

Any unauthorized, inappropriate, illegal or illegitimate use of the University's Information Systems, or failure to comply with this policy will constitute a violation of University policy and will subject the violator to disciplinary action by the University up to and including separation of employment or relationship, and may result in legal action.

For infractions not outlined in an applicable academic honor code or personal conduct code, disciplinary actions will be at the discretion of the Office of Student Conduct (for students), the Department's Chair or Dean and/or Human Resources (for faculty) and/or the Department's manager and/or Human Resources (for staff).

Termination of Access to University Systems and Services

Notwithstanding any other provision of this policy, authorization to access the Information Systems and resources of Liberty University ends at the termination of employment, end of a recognized role or relationship or loss of sponsorship. Electronic mail accounts can be an exception with the understanding that all Liberty Usernames and E-mail accounts are property of Liberty University and as such Liberty University retains exclusive rights to the creation, assignment, revocation, usage and content management of all Liberty Usernames and E-mail accounts.

Confidentiality/Privacy Sections

Electronic Content Property of the University Right of University to Monitor Content

University Information Systems and the messages, e-mail, files attachments, graphics and Internet traffic generated through or within these systems are the property of the University. They are not the private property of any University employee, faculty, staff, contractor, student or any other person. No user of the Information Systems should have an expectation of privacy in their electronic communications. All electronic communications, files and content presented to and/or passed on the Liberty network, including those to, from or through Internet connection(s) may be monitored, examined, saved, read, transcribed, stored or retransmitted by an authorized employee or agent of the University, in its sole discretion, with or without prior notice to the user. The University reserves and intends to exercise the right to do so. Electronic communications and content may also be examined by automated means.

Confidentiality of Content

The confidentiality of any content should not be assumed. Even when a message or material is deleted, it may still be possible to retrieve and read the message or material. Further, use of passwords for security does not guarantee confidentiality. Messages read in HTML may identify the reader to the sender. Aside from the right of the University to retrieve and read any electronic communications or content, such messages or materials must be treated as confidential by other

students or employees and accessed only by the intended recipient. Without prior authorization, no person is permitted to retrieve or read electronic mail messages not sent to them.

Responsibility to Maintain Confidentiality

Notwithstanding the University's right to audit or monitor its Information Systems, all users are required to observe the confidentiality and privacy of others' information accessed through the Information Systems and records of every description, including information pertaining to University programs, students, faculty, staff and affiliates. Without proper authorization, users are not permitted to retrieve or read content not intentionally addressed to them. With proper authorization, the contents of electronic mail or Internet messages or materials may be accessed, monitored, read or disclosed to others within the University or otherwise.

Electronic Privacy Right

The electronic privacy rights of others should be respected at all times while using Information Systems. Use of Information Systems' audio, video, cell phone, "web cam" or related technologies, for the purpose of capturing images and/or recording speech in locations or circumstances where a reasonable expectation of privacy exists is prohibited without the consent of the subject(s) depicted and/or recorded. This provision should not apply to lawful surveillance conducted by law enforcement agencies. The University reserves the right to impose additional restrictions on use of electronic recording devices, in its sole discretion. Questions about the applicability of this provision to a particular situation should be referred to the Office of General Counsel or the Director of Information Security.

Handling of Sensitive Information Disposal of Equipment and Storage Media

Printed materials, computer equipment and storage media containing sensitive and/or protected information should be managed in accordance with published University policies, including Information Disposal Requirements, Asset Disposition procedures, and applicable laws and regulations related to the disposal of hazardous materials.

No Guarantee of Protection Against Unauthorized Access

While the University attempts to protect electronic communication and files from unauthorized access, this cannot be guaranteed. The University is not responsible for the security or privacy of User's personal data stored on Information Systems.

Prohibition on Accessing/Moving Data

Users may not access, copy, or move files including, but not limited to programs, data and electronic mail belonging to another account, without prior authorization from the account

holder. In addition, Users may not access, copy, or move any programs or data files from University's Information System to the User's personal device.

Compliance Sections

Requirement to Comply with Applicable Laws and Policy

The University strives to maintain the security and privacy of electronic communications. Use of University Information Systems or resources, dissemination, and disclosures of information, must comply with the provisions of applicable local, state and federal laws, regulation and University policy.

Lawful Use

Liberty Information Systems may be used for lawful purposes only. It is prohibited to use Liberty Information Systems for unlawful purposes, including, but not limited to the installation of fraudulently or illegally obtained software, harmful software, illegal dissemination of licensed software, sharing of content where the disseminator does not hold lawful intellectual property rights, propagating chain messages, pyramid, ponzi, other unlawful or deceptive schemes, or for any purpose contrary to local, state, federal law or University policy.

Compliance with Copyright Law

Use of University Information Systems must comply with provisions of copyright law and fair use. Copyright law limits the rights of a user to decrypt, copy, edit, transmit or retransmit another's intellectual property, including written materials, images, sounds, music, and performances, even in an educational context, without permission, except where such use is otherwise permitted by this Policy or applicable law.

Compliance with Export Control Regulations

Exports of computing equipment and information technologies from the University must be in compliance with US Export Control Regulations.

Notice of Right to Change Acceptable Use Policy

The University reserves the right to change this policy or any portion of the policy, at any time, with or without prior notice. Changes to this policy are effective upon posting in the University Policy Directory, where the most current version resides. The AUP was last revised on July 28, 2020. This policy replaced previous PG0017.

Sanctions

The University regards any violation of this Policy as a serious offense, which may result in an investigation and enforcement action consistent with established University disciplinary policies and procedures. Users who violate this Policy are subject to sanctions ranging from denial of access to any or all Information Systems up to and including termination (for an employee), dismissal (for a student), or loss of access (for a guest). Violators may also be referred for prosecution under applicable local, state or federal laws. The University reserves the right to withhold computing privileges from those who do not abide by both the letter and spirt of this Policy.

Related Policies

Information Services has adopted additional policies regarding hardware, software, computer use, internet use, and associated guidance information related to the use of the Information Systems. Employees must comply with this Policy, in addition to all other Information Services policies. Please access the following web site for a complete list of Information Services policies: https://www.liberty.edu/index.cfm?PID=20998.

Affected Parties

All University Students, Faculty, Staff and Alumni

Policy Language

Liberty University utilizes multi-factor authentication for network access to privileged accounts and non-privileged accounts.

Policy Rationale

The purpose of this policy is to define requirements for accessing Liberty University's network and information systems whether on or off campus. These standards are designed to minimize the potential security exposure to Liberty University from damages that may result from unauthorized access of the university's resources. Multifactor authentication adds a layer of security which helps deter the use of compromised credentials. Cyber criminals and attackers are becoming more advanced in their efforts to not only steal information, but also modify data, delete data, spread malicious code, harvest credentials, and distribute spam. No organization regardless of size is exempt from such attacks. Password theft has also been on the rise with the use of methods such as key logging, phishing, and pharming. Requiring an additional layer of authentication helps reduce the risk of a compromise.

For additional information, please visit the University's Multi-Factor Authentication webpage.

Definition of Glossary Terms

Key logging - Recording a log of keystrokes on a computer in order to gain access to passwords and other confidential information

Multi-factor authentication (MFA) - Requiring two or more authentication methods for a secure login. Authentication factors are typically something you know (knowledge factor), something you have (possession factor) and something you are (inherence factor).

Phishing - Sending emails appearing to be from a reputable company in an effort to acquire personal information under false pretenses

Pharming - Sending internet users to a false website that mimics a legitimate one

PROCEDURES

Secure all individual non-console administrative access and all remote access to sensitive data using multi-factor authentication for every session.

Incorporate multi-factor authentication for all network access, both privileged accounts and non-privileged accounts.

1. The multi-factor authentication should be device specific and need not be required at every login, but on the first login of any new device, and again every 75 days after initial device multi-factor authentication, or upon suspicious changes to the login session.

2. Passwords must still be required at every login or after a session timeout.

Exceptions

Exceptions for active military personnel can be granted on a case-by-case basis.

No exceptions allowed for Faculty/Staff members.

Initial Approval Date

6/25/2018

Date of Last Review

8/14/2023

Date for Review

8/14/2028